

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-308264

(43)Date of publication of application : 05.11.1999

(51)Int.Cl.

H04L 12/46

H04L 12/28

G06F 13/00

H04L 9/08

H04L 9/14

H04L 9/36

H04L 12/66

H04L 12/56

(21)Application number : 10-107808

(71)Applicant : MITSUBISHI ELECTRIC CORP

(22)Date of filing : 17.04.1998

(72)Inventor : NAGASHIMA NORIMITSU

INADA TORU

IDEGUCHI TETSUO

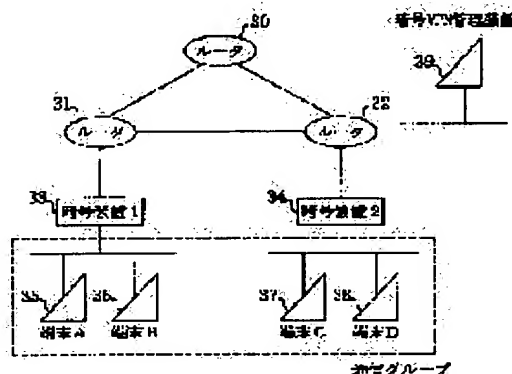
WATANABE AKIRA

(54) CRYPTOCOMMUNICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To reduce a load on a network manager at the time of setting a cipher device and to eliminate an overhead at the time of starting cryptographic communication by specifying a communication group using a block diagram of the network, obtaining a communication path of a communication terminal, preparing a cryptographic communication control table and distributing it to the cipher device.

SOLUTION: A cipher VPN management device 39 selects a cipher device which communicates by using a network block diagram, specifies a communication group, obtains communication path for communication terminals 35 to 38 of the specified communication group, prepares a cryptographic communication control table to be distributed to cipher device 33 and 34. Thus, the communication paths are clarified in the communication between the communication terminals 35 and 38 and operation mistakes by manually setting cryptographic communication information are made fewer. Also, when communication data from the terminals 35 to 38 are received, it is possible to eliminate an overhead at the time of starting the cryptographic communication since the cipher device 33 and 34 hold the cryptographic communication control table and there is no need to transmit a key search packet.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

THIS PAGE BLANK (USPTO)

[Kind of final disposal of application other than
the examiner's decision of rejection or
application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

2004.07.07 10:00:00

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-308264

(43) 公開日 平成11年(1999)11月5日

(51) Int.Cl. ⁸	識別記号	F I	
H 0 4 L 12/46		H 0 4 L 11/00	3 1 0 C
12/28		G 0 6 F 13/00	3 5 1 Z
G 0 6 F 13/00	3 5 1	H 0 4 L 9/00	6 0 1 Z
H 0 4 L 9/08			6 4 1
9/14			6 8 5

審査請求 未請求 請求項の数 4 O L (全 13 頁) 最終頁に続く

(21) 出願番号 特願平10-107808

(22) 出願日 平成10年(1998)4月17日

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 永島 規充

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(72) 発明者 稲田 徹

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(72) 発明者 井手口 哲夫

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(74) 代理人 弁理士 宮田 金雄 (外2名)

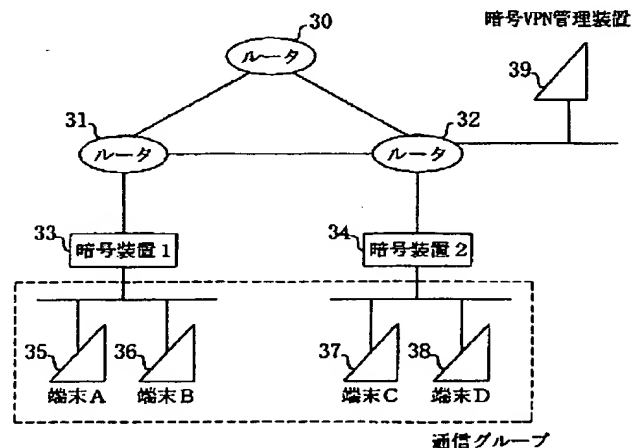
最終頁に続く

(54) 【発明の名称】 暗号通信システム

(57) 【要約】

【課題】 大規模ネットワークにおいても暗号通信のためのネットワーク管理を容易にし、かつ暗号通信時のオーバーヘッドをなくし、暗号通信経路を明確化する。

【解決手段】 ネットワーク構成図を暗号VPN管理装置に表示、構成図上で暗号通信グループを指定し、通信グループ内のすべての端末の通信経路を検索し、通信経路上にある暗号装置の暗号通信制御テーブルを作成し、暗号装置に配送する。



【特許請求の範囲】

【請求項1】 通信ネットワークに収容された複数の通信端末と、それら通信端末間でやり取りするデータを中継、暗号化する暗号装置と、それら暗号装置からのデータを中継するルータとを有する通信ネットワークを構成し、この通信ネットワークを仮想的な私設ネットワークとしてみなしてVPN (Virtual Private Network) を管理する暗号VPN管理装置とを有する暗号通信システムにおいて、
前記暗号VPN管理装置は、ルータ、通信端末及び暗号装置等のネットワーク構成図を表示する構成図表示手段と、この構成図に基づいて、通信エリア、通信端末、通信端末群あるいは暗号装置を選択して通信グループを指定する通信グループ指定手段と、
この指定された通信グループに属する通信端末間の暗号通信において使用する鍵IDを設定する鍵ID設定手段と、
前記通信グループに属する通信端末間のすべての通信経路を検索し、検索結果に基づいて各通信経路に対する暗号装置の処理を決定し、通信経路の送信元、宛先アドレス、通信データを暗号化、透過あるいは廃棄するかを示す制御コード及び暗号鍵IDを含む暗号通信制御テーブルを通信経路上の前記暗号装置毎に作成する暗号通信制御テーブル作成手段と、
これを各暗号装置に配送する配送手段を有し、
前記暗号装置は、受け取った前記暗号通信制御テーブルに基づいて通信データを処理する通信データ処理手段を有することを特徴とする暗号通信システム。

【請求項2】 通信ネットワークに収容された複数の通信端末と、それら通信端末間でやり取りするデータを中継、暗号化する暗号装置と、それら暗号装置からのデータを中継するルータとを有する通信ネットワークを構成し、この通信ネットワークを仮想的な私設ネットワークとしてみなしてVPN (Virtual Private Network) を管理する暗号VPN管理装置とを有する暗号通信システムにおいて、
前記暗号VPN管理装置は、ルータ、通信端末及び暗号装置等のネットワーク構成図を表示する構成図表示手段と、この構成図に基づいて、通信エリア、通信端末、通信端末群あるいは暗号装置を選択して通信グループを指定する通信グループ指定手段と、
前記通信グループに属する通信端末間のすべての通信経路を検索し、検索結果に基づいて各通信経路に対する暗号装置の処理を決定し、通信経路の送信元、宛先アドレス、通信データを暗号化、透過あるいは廃棄するかを示す制御コードを含む暗号通信制御テーブルを通信経路上の暗号装置毎に作成する暗号通信制御テーブル作成手段と、制御コードが暗号の場合には暗号鍵を生成して前記暗号通信制御テーブルに設定する暗号鍵設定手段と、

これを各暗号装置に配送する配送手段とを有し、
前記暗号装置は、受け取った前記暗号通信テーブル及び暗号鍵に基づいて通信データを処理する通信データ処理手段を有することを特徴とする暗号通信システム。

【請求項3】 前記通信グループ指定手段により指定された通信グループに属する通信端末間のすべての通信経路を検索して、各通信路においてデータ暗号化、復号を行う暗号装置が決定できない場合、指定した通信グループ内の通信が平文で行われることを示す確認メッセージを表示する確認メッセージ表示手段と確認結果に応じて暗号装置の処理を決定する処理決定手段を有することを特徴とする請求項1または請求項2に記載の暗号通信システム。

【請求項4】 前記暗号VPN管理装置の暗号通信制御テーブル作成手段は、通信グループに対するセキュリティレベルを設定し、指定された通信グループが他の通信グループと重複する場合、前記設定されたセキュリティレベルに基づいて暗号通信制御テーブルを作成することを特徴とする請求項1または請求項2に記載の暗号通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、コンピュータネットワークにおけるデータの機密を保持する暗号通信システムに関する。

【0002】

【従来の技術】近年のコンピュータネットワークの普及に伴い、ネットワーク上のデータの機密を保持する通信データ暗号技術への関心が高まっている。従来、通信データの暗号については特開平6-209313に見られるように、暗号装置内部に保持している通信データの宛先、送信元アドレスの一方あるいはその両方に対応した暗号鍵を登録した暗号テーブルに従ってデータを暗号化、復号する方法がとられていた。しかし、暗号テーブルは、各暗号装置毎に異なるためネットワーク管理者はネットワークの構成及び通信端末のアドレスを考慮して各暗号装置に対応する暗号テーブルを作成する必要がある、特に、ネットワークが大規模になると通信端末数も増大し、暗号テーブルが非常に複雑になるという課題があった。

【0003】この課題を解決するため、特願平9-143755 暗号通信システムのように、図15のようなネットワーク構成において暗号鍵探索パケット(図17)を用いて、通信端末間の通信経路上の暗号装置の暗号鍵情報を収集し、収集した暗号鍵情報に基づいて暗号鍵情報を自動的に図16のような暗号鍵テーブルに学習し、通信端末間の通信データを各暗号装置が暗号化、復号、平文中継する方法がとられた。

【0004】

【発明が解決しようとする課題】上述の方法では、通信

端末間で最初にデータ通信を始める場合、暗号鍵テーブル作成のため図17に示される暗号鍵探索パケットが送信され、この暗号鍵探索パケットに対する応答を受け取ってからでないと、暗号通信が行えないため通信開始までのオーバーヘッドが大きくなる問題があった。また、上述の方法では暗号装置が暗号鍵探索パケットを用いて、自動的に暗号鍵情報を収集、登録してしまうため、ネットワーク管理者が実際の通信の途中経路を把握することができない。さらに、インターネットを介してLANを接続するようなケースでは、暗号鍵探索パケットが暗号化されずにインターネット上を流れることになり、ファイアウォールなどで守られた企業ネットワークに、インターネットからの鍵探索パケットを通過させるのは安全性の問題があった。

【0005】本発明は、このような暗号通信開始時のオーバーヘッド、暗号通信経路の明確化及び企業ネットワークへの安全性に対応するためになされたもので、ネットワーク構成図を用いて、暗号通信のエリア、通信端末群が指定でき、暗号装置の接続箇所、通信端末間の通信における通信経路を明示して、暗号装置の設定時のネットワーク管理者の負荷を軽減すると共に暗号通信開始時のオーバーヘッドをなくし、また企業ネットワークの安全性を損なうことなく暗号通信を実現することを目的としている。

【0006】

【課題を解決するための手段】第1の発明に係る暗号通信システムは、通信ネットワークに収容された複数の通信端末と、それら通信端末間でやり取りするデータを中継、暗号化する暗号装置と、それら暗号装置からのデータを中継するルータとを有する通信ネットワークを構成し、この通信ネットワークを仮想的な私設ネットワークとしてみなしてVPN (Virtual Private Network) を管理する暗号VPN管理装置とを有する暗号通信システムにおいて、前記暗号VPN管理装置は、ルータ、通信端末及び暗号装置等のネットワーク構成図を表示する構成図表示手段と、この構成図に基づいて、通信エリア、通信端末、通信端末群あるいは暗号装置を選択して通信グループを指定する通信グループ指定手段と、この指定された通信グループに属する通信端末間の暗号通信において使用する鍵IDを設定する鍵ID設定手段と、前記通信グループに属する通信端末間のすべての通信経路を検索し、検索結果に基づいて各通信経路に対する暗号装置の処理を決定し、通信経路の送信元、宛先アドレス、通信データを暗号化、透過あるいは廃棄するかを示す制御コード及び暗号鍵IDを含む暗号通信制御テーブルを通信経路上の前記暗号装置毎に作成する暗号通信制御テーブル作成手段と、これを各暗号装置に配送する配送手段を有し、前記暗号装置は、受け取った前記暗号通信制御テーブルに基づいて通信データを処理する通信データ処理手段を有するものである。

【0007】第2の発明に係る暗号通信システムは、通信ネットワークに収容された複数の通信端末と、それら通信端末間でやり取りするデータを中継、暗号化する暗号装置と、それら暗号装置からのデータを中継するルータとを有する通信ネットワークを構成し、この通信ネットワークを仮想的な私設ネットワークとしてみなしてVPN (Virtual Private Network) を管理する暗号VPN管理装置とを有する暗号通信システムにおいて、前記暗号VPN管理装置は、ルータ、通信端末及び暗号装置等のネットワーク構成図を表示する構成図表示手段と、この構成図に基づいて、通信エリア、通信端末、通信端末群あるいは暗号装置を選択して通信グループを指定する通信グループ指定手段と、前記通信グループに属する通信端末間のすべての通信経路を検索し、検索結果に基づいて各通信経路に対する暗号装置の処理を決定し、通信経路の送信元、宛先アドレス、通信データを暗号化、透過あるいは廃棄するかを示す制御コードを含む暗号通信制御テーブルを通信経路上の暗号装置毎に作成する暗号通信制御テーブル作成手段と、制御コードが暗号の場合には暗号鍵を生成して前記暗号通信制御テーブルに設定する暗号鍵設定手段と、これを各暗号装置に配送する配送手段とを有し、前記暗号装置は、受け取った前記暗号通信テーブル及び暗号鍵に基づいて通信データを処理するものである。

【0008】第3の発明に係る暗号通信システムは、前記通信グループ指定手段により指定された通信グループに属する通信端末間のすべての通信経路を検索して、各通信路においてデータ暗号化、復号を行う暗号装置が決定できない場合、指定した通信グループ内の通信が平文で行われることを示す確認メッセージを表示する確認メッセージ表示手段と、確認結果に応じて暗号装置の処理を決定する処理決定手段を有するものである。

【0009】第4の発明に係る暗号通信システムは、前記暗号VPN管理装置の暗号通信制御テーブル作成手段は、通信グループに対するセキュリティレベルを設定し、指定された通信グループが他の通信グループと重複する場合、前記設定されたセキュリティレベルに基づいて暗号通信制御テーブルを作成するものである。

【0010】

【発明の実施の形態】実施の形態1. 図1は、実施の形態1におけるネットワーク構成の例で、ルータ3台(30~32)、暗号装置1、2(33、34)、通信端末A、B、C、D(35~38)及び暗号VPN管理装置(39)が接続されている。図2はこの発明の暗号通信システムを構成する暗号VPN管理装置であり、図2において、1は、暗号装置を管理する暗号VPN管理装置、2は送受信処理部で、通信データの受信処理、送信処理を実施し、3はキーボード、マウスの入力を制御する入力制御部、4はルータ、暗号装置及び通信端末等のネットワーク機器の構成図を表示する構成表示部、5は

ネットワーク構成図上でネットワーク管理者によって指定された通信グループの情報から暗号通信制御テーブルを生成する暗号テーブル演算部、6は前記暗号通信制御テーブルを暗号化する暗号処理部、7は暗号処理部6で暗号化された暗号通信制御テーブルを暗号装置に配送する配送処理部である。

【0011】図3は、この発明の暗号通信システムを構成する暗号装置である。図3において10は暗号装置、13は通信データを暗号化、復号する暗号化・復号部、14は通信データを透過的に中継する透過中継部、15は通信データを廃棄する廃棄部、17は暗号VPN管理装置で作成、送信された暗号通信制御テーブルを受信するテーブル管理部、18は前記受信した暗号通信制御テーブルを復号する復号部、16は通信データの処理方法を示す暗号通信制御テーブル、11はパブリックポート、20はローカルポートである。これらのポートは暗号装置が通信データを暗号化するか復号するかを識別するもので、暗号装置はパブリックポート11から受信した通信データを復号し、ローカルポート20に送信し、ローカルポート20から受信した通信データを暗号化し、パブリックポート11に送信する。12、19は送受信処理部で通信データの受信処理、送信処理を実施する。

【0012】次に図6を用いて動作について説明する。まずネットワーク管理者が暗号VPN管理装置の構成表示部4を起動し、図1のようなネットワーク構成図を表示する(ステップ1)。構成表示部4は、ネットワーク管理者による手入力もしくはSNMP(Simple Network Management Protocol)を用いて収集した情報を元にネットワーク構成図を表示する。次に、ネットワーク管理者は、マウス、キーボードを使用して通信を行う暗号装置(この例では暗号装置1、2(33、34))を選択し、通信グループを指定する(ステップ2)。本実施例の場合、暗号装置の下流に接続されているネットワークを通信グループとする。暗号装置で使用する暗号鍵ID(この例では暗号鍵ID=1)を入力する(ステップ3)。入力制御部3は、画面のどの暗号装置が選択されたかを構成表示部4に通知する。構成表示部4は、通知された情報を元にネットワーク管理者が指定した通信グループに属するすべての通信端末、暗号装置のアドレス情報、通信経路及び暗号鍵IDをテーブル演算部5に通知する。テーブル演算部5では、通知された通信経路から1つを取り出し(例えば、通信端末A(35)ー暗号装置1(33)ールータ(31)ールータ(32)ー暗号装置2(34)ー通信端末C(37))、この通信経路にある暗号装置に対して(例:暗号装置1(33))、まずこの暗号装置がネットワーク管理者がステップ2で選択した暗号装置かチェックする(ステップ6)。選択した暗号装置でない場合は、通信経路の両端のアドレスをこの暗号装置の暗号通信制御テーブルの宛

先、送信元アドレスに設定し、制御コードに透過中継を設定する(ステップ7)。ネットワーク管理者が選択した暗号装置の場合は、通信経路上にネットワーク管理者が選択した別の暗号装置が存在するかチェックし(ステップ8)、存在すれば、暗号通信制御テーブルに通信経路の両端のアドレスを設定し、制御コードを暗号、暗号鍵IDにステップ3で入力されたものを設定し(ステップ10)、図4のような暗号通信制御テーブル16を作成する。存在しない場合は、制御コードを廃棄とし、暗号通信制御テーブルに設定する(ステップ9)。これを1つの通信経路に存在する暗号装置分(前記通信経路の場合は、経路上に存在する暗号装置の数は2である)処理する(ステップ5)。このステップ5~10の処理を通知されたすべての通信経路分(図1のネットワーク構成での通信経路は、

経路1:通信端末A(35)ー暗号装置1(33)ールータ(31)ールータ(32)ー暗号装置2(34)ー通信端末C(37)

経路2:通信端末B(36)ー暗号装置1(33)ールータ(31)ールータ(32)ー暗号装置2(34)ー通信端末C(37)

経路3:通信端末A(35)ー暗号装置1(33)ールータ(31)ールータ(32)ー暗号装置2(34)ー通信端末D(38)

経路4:通信端末B(36)ー暗号装置1(33)ールータ(31)ールータ(32)ー暗号装置2(34)ー通信端末D(38)

経路5:通信端末A(35)ー通信端末B(36)

経路6:通信端末C(37)ー通信端末D(38)

の6経路である)行い(ステップ4)、各暗号装置に対する暗号通信制御テーブル16(図4)を完成させ、暗号処理部6でこれを暗号化し(ステップ11)、テーブル配送部7、送受信処理部2を経由し、図5のようなフォーマットで暗号VPN管理装置39から暗号装置1、2(33、34)へ、暗号通信制御テーブル16(図4)を配送する(ステップ12)。

【0013】配送された暗号通信制御テーブル16(図4)は、暗号装置のローカルポート20またはパブリックポート11で受信され、テーブル復号部18でデータを復号後、テーブル管理部17で処理され、暗号装置内部に保存される。以降、暗号装置では、通信データを受信する度に、暗号通信制御テーブル16を参照し、通信データの宛先、送信元アドレスが暗号通信制御テーブル内と一致した場合、制御コードに従い、制御コードが暗号となっている時は保持している暗号鍵の中から暗号鍵IDに対応する暗号鍵で通信データを暗号化、復号する。制御コードが透過中継となっている場合は、データをそのまま中継する。通信データの宛先、送信元アドレスが暗号通信制御テーブルと一致しない場合は、データを廃棄する。

【0014】以上のように、暗号VPN管理装置でネットワーク構成図を用いて、通信する暗号装置を選択し、通信グループを指定し、指定された通信グループの通信端末のすべての通信経路を求め、暗号通信制御テーブルを作成し、暗号装置に配送するようにしているので、通信端末間の通信における通信経路が明確化され、通信端末のアドレスを元に人手により暗号通信情報を設定するより操作ミスを少なくできる。通信端末からの通信データを受信した場合も、暗号装置は暗号通信制御テーブル16を保持しているため、鍵探索パケットを送信する必要がないので暗号通信開始時のオーバーヘッドをなくすることができ、また企業ネットワークの安全性を損なうことなく暗号通信を実現することができる。上記例では、ネットワーク管理者がネットワーク構成図上で通信する暗号装置を選択しているが、図1の点線部のようにマウスで通信端末、通信端末群あるいはエリアを囲み通信グループを指定しても同様の効果を得ることができる。

【0015】実施の形態2。実施の形態1では、暗号VPN管理装置から暗号鍵IDを含む暗号通信制御テーブルを配送する場合の例を示したが、本実施の形態では、次に暗号鍵IDの代わりに暗号鍵を配送する場合の実施の形態を示す。図7は、この実施の形態2における暗号VPN管理装置であり、図2に暗号鍵を生成する暗号鍵生成部52を追加したものである。暗号装置は図2、ネットワーク構成は図1と同様である。次に動作について図9を用いて説明する。ネットワーク管理者が通信グループを指定し、指定された情報を元に暗号通信制御テーブル16（図8）を作成するまでの手順（ステップ1、3～9）は前記実施の形態1と同様であるが、ステップ8で通信経路上にネットワーク管理者が指定した暗号装置が存在する場合に、暗号通信制御テーブルに通信経路の両端の通信端末のアドレス及び制御コードに暗号を設定し（ステップ13）、暗号鍵生成部において暗号鍵を生成し（ステップ14）、図8に示されるような暗号通信制御テーブルに設定し、暗号装置へ送信する（ステップ11、12）。

【0016】暗号装置では送付された暗号鍵を含む暗号通信制御テーブルを暗号装置内部に保存し、以降、通信データを受信する度に、暗号通信制御テーブル16（図8）を参照し、通信データの宛先、送信元アドレスが暗号通信制御テーブル内と一致した場合、制御コードに従い、コードが暗号となっている場合は、暗号通信制御テーブルにある暗号鍵で通信データを暗号化、復号する。制御コードが透過中継及び廃棄となっている場合は、実施の形態1と同様である。

【0017】以上のように、暗号VPN管理装置から暗号鍵も合わせて配送するようにしているので、暗号鍵IDの重複や数の制限を無くし、保持している暗号鍵のリストが異なっているため鍵IDが合っているにもかかわらず通信できないといった通信の不通状態を防ぐことが

できる。また、実施の形態1の効果が得られることは言うまでもない。以上の実施の形態2では、ネットワーク管理者がネットワーク構成図上で暗号装置を選択しているが、通信端末あるいはエリアを選択し、通信グループを指定することでも同様の効果を得ることができる。

【0018】実施の形態3。実施の形態1では、ネットワーク管理者が通信を行う暗号装置を選択するようにしたものであるが、本実施の形態は暗号装置が接続されていない通信端末と通信する場合の実施の形態を示す。図10は、本実施の形態におけるネットワーク構成図である。次に動作を図12を用いて説明する。通信端末C、D（37、38）側に暗号装置は接続されていないので、ネットワーク管理者は、構成図上で暗号装置1（33）と通信端末C、D（37、38）を選択し、通信グループを指定する（ステップ1、2）。以降のステップ3～8は図9と同様である。ステップ8では、通信経路上にネットワーク管理者が指定した暗号装置が存在するかチェックするが、暗号装置が存在しないので、ネットワーク管理者に対し、この通信経路における通信が透過中継になることの確認メッセージを表示し（ステップ15）。応答がYes場合は、制御コードを透過中継とし暗号通信制御テーブル16（図11）を設定する（ステップ7）。Noの場合は、制御コードを廃棄として暗号通信制御テーブルを設定し、（ステップ9）、暗号装置へ配送する（ステップ11、12）。暗号装置の動作は、実施の形態1、2と同様である。

【0019】以上のように、ネットワーク管理者が指定した通信グループ内の通信が透過中継となる場合に、ネットワーク管理者へ問い合わせるため、セキュリティが低下することを確認でき、誤って通信グループを指定してしまった場合にも事前に検出できる。

【0020】実施の形態4。実施の形態3では、ネットワーク管理者が指定する通信グループが他の通信グループと重複していないが、本実施の形態では、重複する場合の実施の形態を以下に示す。図13は、ネットワーク管理者が指定した複数の通信グループが重複するような場合のネットワーク構成図である。次に図14を用いて動作を説明する。ネットワーク管理者は、ネットワーク構成図を表示し（ステップ1）、ネットワーク構成図上のエリア、通信端末及び暗号装置を選択し、通信グループ1を指定し（ステップ2）、この通信グループのセキュリティレベル（図の例では=1）を設定する。続いて、前記と同様の手順で通信グループ2、セキュリティレベル=2を設定する（ステップ2、16）。通信グループの指定が終了したら（ステップ17）、前記実施の形態と同様にすべての通信経路を検索し、通信経路にある暗号装置に対して、同一セキュリティレベルの通信グループに属する暗号装置が存在するかチェックする（ステップ18）。同じレベル暗号装置がない存在しない場合は、通信経路の両端のアドレスをこの暗号装置の暗号

通信制御テーブルの宛先、送信元アドレスに設定し、制御コードに廃棄を設定する(ステップ9)、存在する場合は、暗号通信制御テーブルに通信経路の両端のアドレス、制御コードに暗号を設定し(ステップ13)、暗号鍵を生成して暗号通信制御テーブルに設定し(ステップ14)、暗号装置へ配送する(ステップ11、12)。暗号装置の動作は、実施の形態1と同様である。

【0021】以上のように、ネットワーク管理者が指定する通信グループにセキュリティレベルを設け、通信グループが重複する場合、セキュリティレベルを比較するので、暗号通信グループの設定が柔軟になり、また、通信グループが重複しても通信端末間通信のセキュリティを保つことができる。

【0022】

【発明の効果】以上のように、第1の発明によれば、暗号VPN管理装置に表示されたネットワーク構成図を使用して通信グループを指定し、通信端末の通信経路を求め、暗号通信制御テーブルを作成し、暗号装置に配送するようにしているので、通信端末間の通信における通信経路が明確化され、通信端末のアドレスを元に人手により暗号通信情報を設定するより操作ミスを少なくできる。通信端末からの通信データを受信した場合も、暗号装置は暗号通信テーブルを保持しているため、鍵探索パケットを送信する必要がないので暗号通信開始時のオーバーヘッドをなくすことができ、また企業ネットワークの安全性を損なうことなく暗号通信を実現できる。

【0023】第2の発明によれば、暗号VPN管理装置から暗号通信制御テーブルと暗号鍵を合わせて配送するようにしているので、保持している鍵が異なっているため鍵IDが合っているにもかかわらず通信できないといった通信の不通状態を防ぐことができる。

【0024】第3の発明によれば、ネットワーク管理者は指定した通信グループ内の通信が透過中継となる場合に、問い合わせるため、ネットワーク管理者はセキュリティが低下することを確認でき、誤ってエリア、通信端末を指定してしまった際にも事前に検出できる。

【0025】第4の発明によれば、ネットワーク管理者が指定する通信グループにセキュリティレベルを設け、通信グループが重複する場合、セキュリティレベルを比較するので、暗号通信グループの設定が柔軟になり、また、通信グループが重複しても通信端末間通信のセキュリティを保つことができる。

【図面の簡単な説明】

【図1】 実施の形態1、2におけるネットワーク構成図である。

【図2】 実施の形態1の暗号VPN管理装置を示すブロック図である。

【図3】 この発明の暗号装置を示すブロック図である。

【図4】 実施の形態1の暗号装置1における暗号通信

制御テーブルである。

【図5】 この発明の管理通信フレームである。

【図6】 実施の形態1における暗号VPN管理装置の処理を示すフローチャートである。

【図7】 実施の形態2の暗号VPN管理装置を示すブロック図である。

【図8】 実施の形態2の暗号装置1における暗号通信制御テーブルである。

【図9】 実施の形態2における暗号VPN管理装置の処理を示すフローチャートである。

【図10】 実施の形態3におけるネットワーク構成図である。

【図11】 実施の形態3の暗号装置1における暗号通信制御テーブルである。

【図12】 実施の形態3における暗号VPN管理装置の処理を示すフローチャートである。

【図13】 実施の形態4におけるネットワーク構成図である。

【図14】 実施の形態4における暗号VPN管理装置の処理を示すフローチャートである。

【図15】 従来例における暗号通信の接続図である。

【図16】 従来例における暗号鍵テーブルである。

【図17】 従来例における鍵探索パケットである。

【符号の説明】

1 暗号VPN管理装置

2 送受信処理部

3 入力制御部

4 構成表示部

5 テーブル演算部

6 暗号処理部

7 テーブル配送部

10、33、34、60、61、71、72、73、

74、75 暗号装置

11 パブリックポート

12、19 送受信処理部

13 暗号化、復号部

14 透過中継部

15 廃棄部

16 暗号通信制御テーブル

17 テーブル管理部

18 テーブル復号部

19 ローカルポート

30、32 ルータ

31、36、37、38、76、77、78 通信端末

39 暗号VPN管理装置

52 暗号鍵生成部

81 ヘッダ

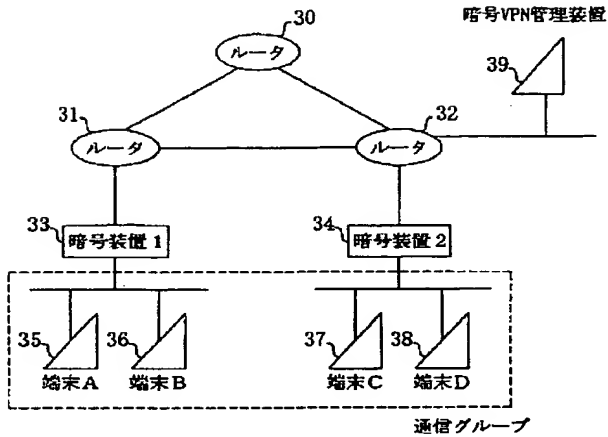
82 送信元端末アドレス

83 宛先端末アドレス

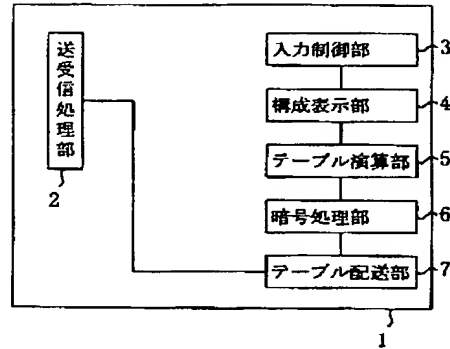
- 84 ローカルポート暗号鍵情報
85 パブリックポート暗号鍵情報

- 91 ヘッダ
92 暗号通信制御テーブル

【図1】

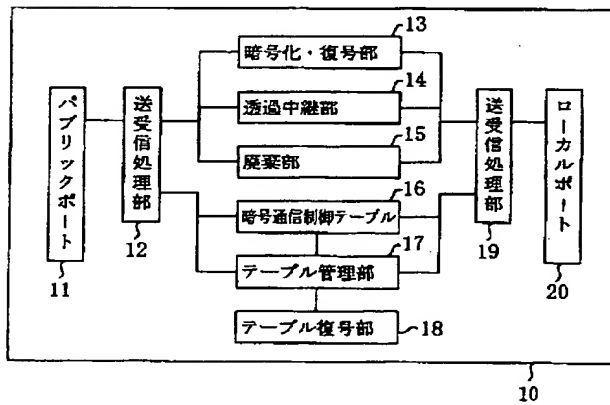


【図2】



【図4】

【図3】



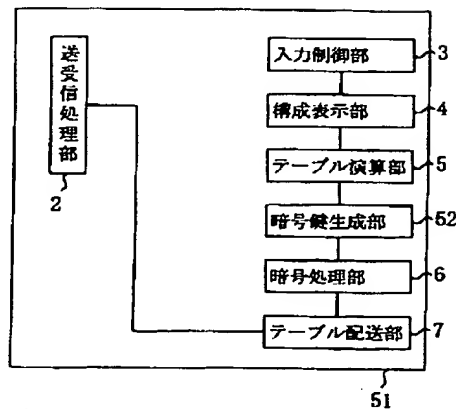
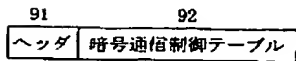
宛先	送信元	制御コード	暗号鍵ID
C	A	暗号	1
D	B	暗号	1
C	B	暗号	1
D	A	暗号	1

【図8】

宛先	送信元	制御コード
C	A	暗号
D	B	暗号
C	B	暗号
D	A	暗号
暗号鍵		

【図5】

【図7】



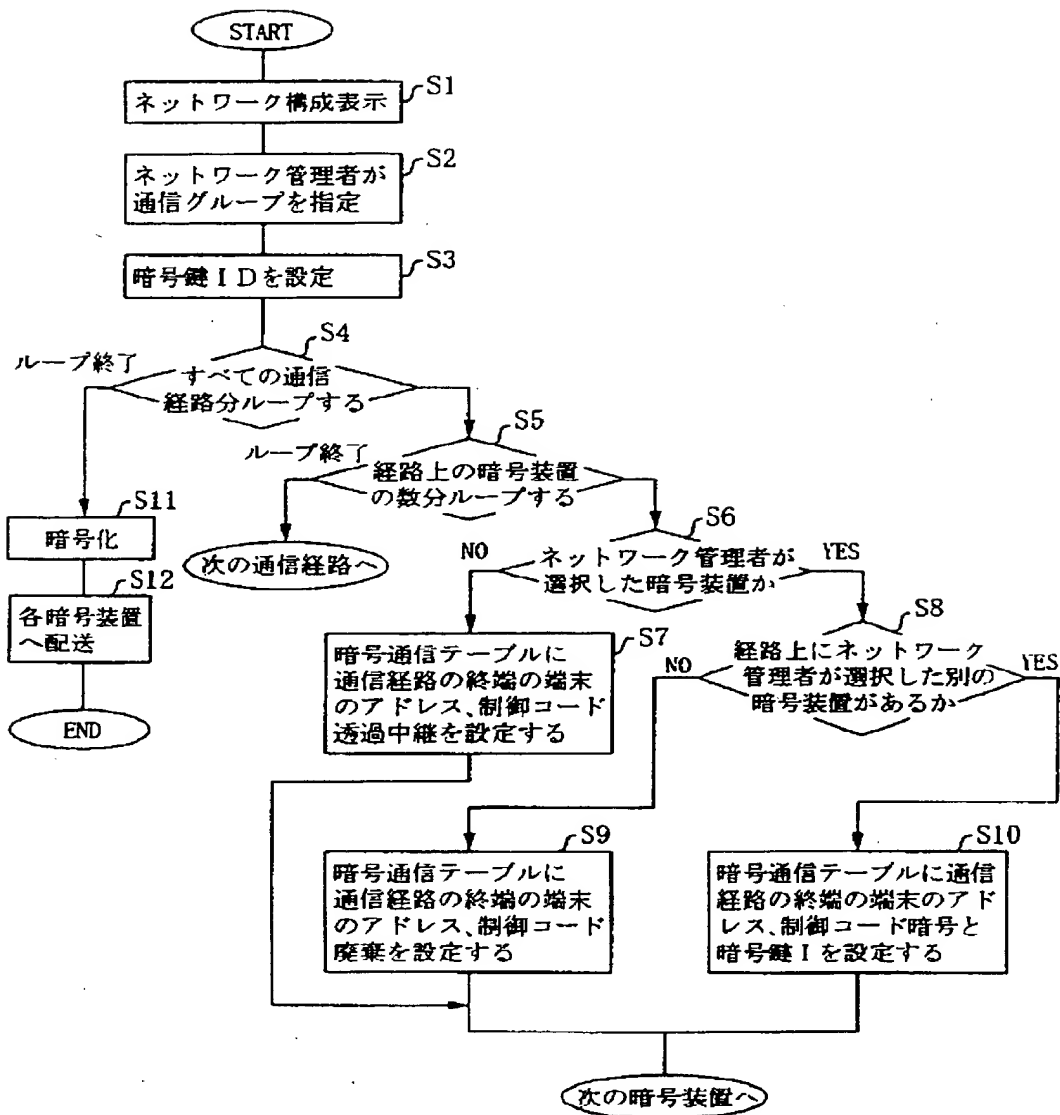
【図11】

宛先	送信元	制御コード
C	A	透過中継
D	B	透過中継
C	B	透過中継
D	A	透過中継

【図16】

通信端末	処理方法	保持時間
A-B	ID 1	600
A-C	廃棄	600

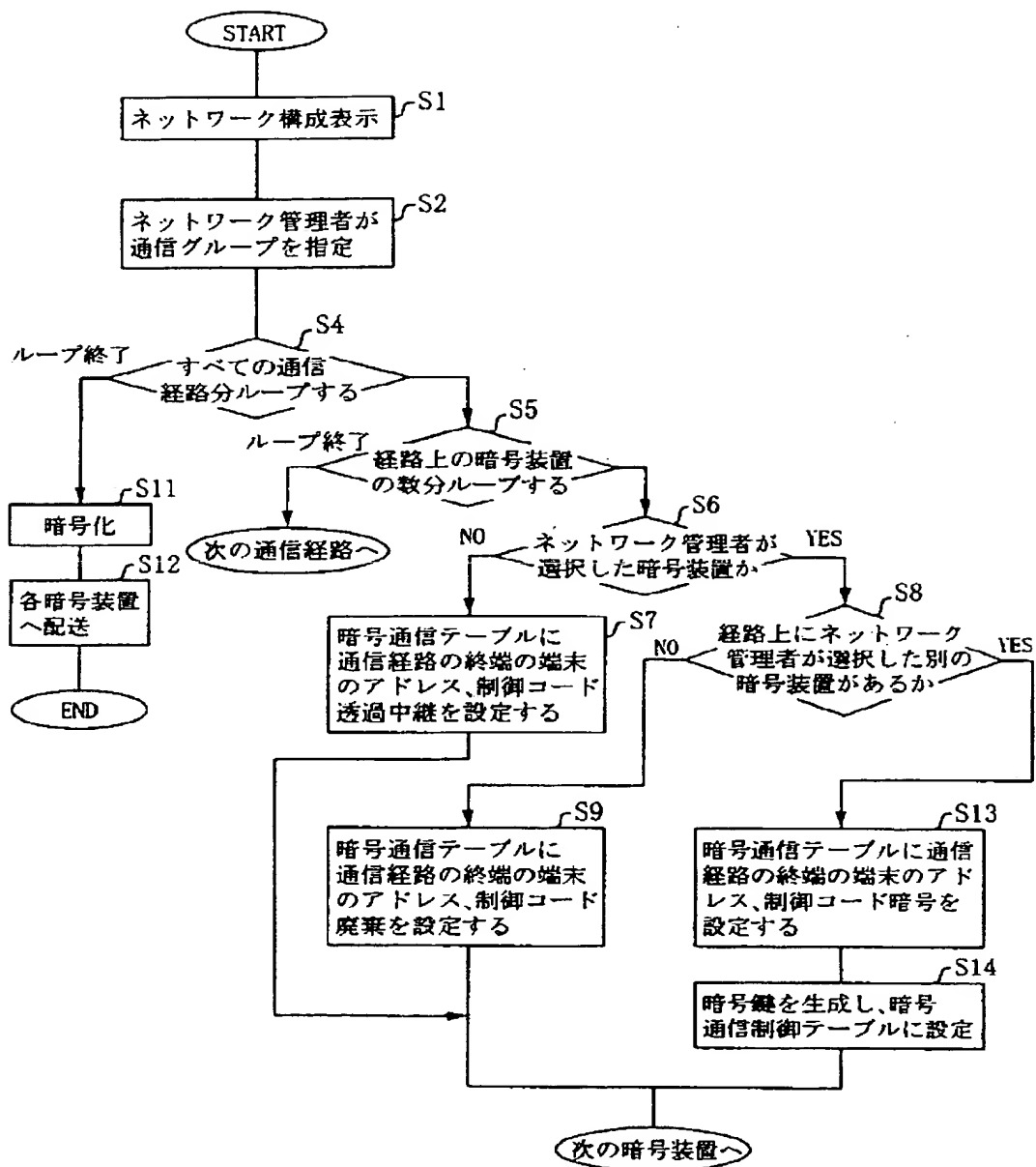
【図6】



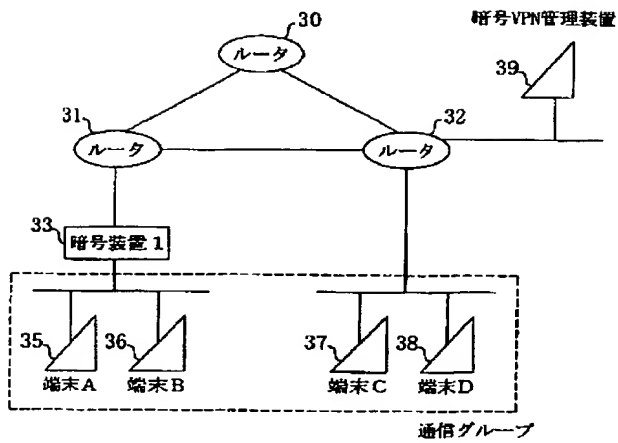
【図17】

81	82	84	85
ヘッダ	送信元端末 アドレス	宛先端末 アドレス	ローカルポート 暗号鍵情報
			パブリックポート 暗号鍵情報

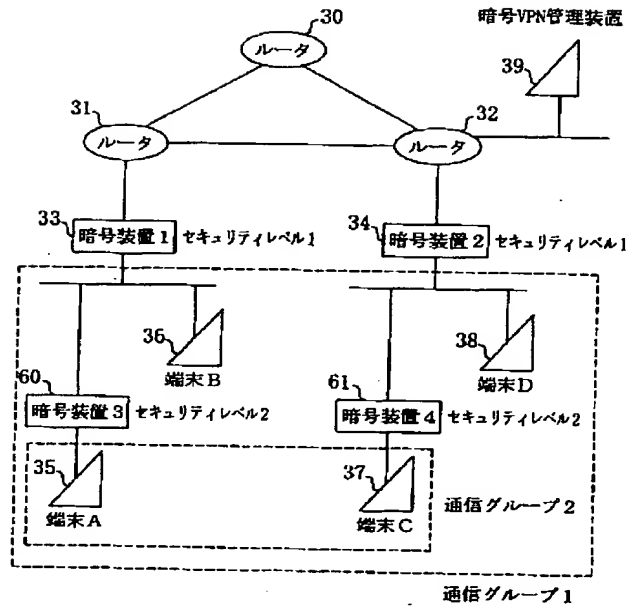
【図9】



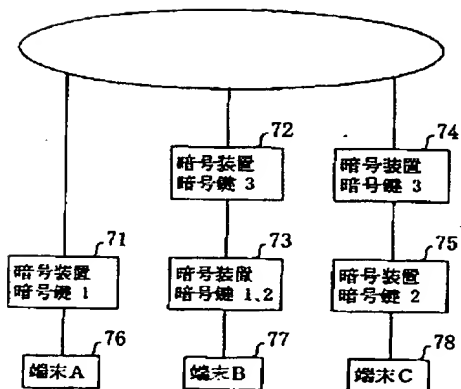
【図10】



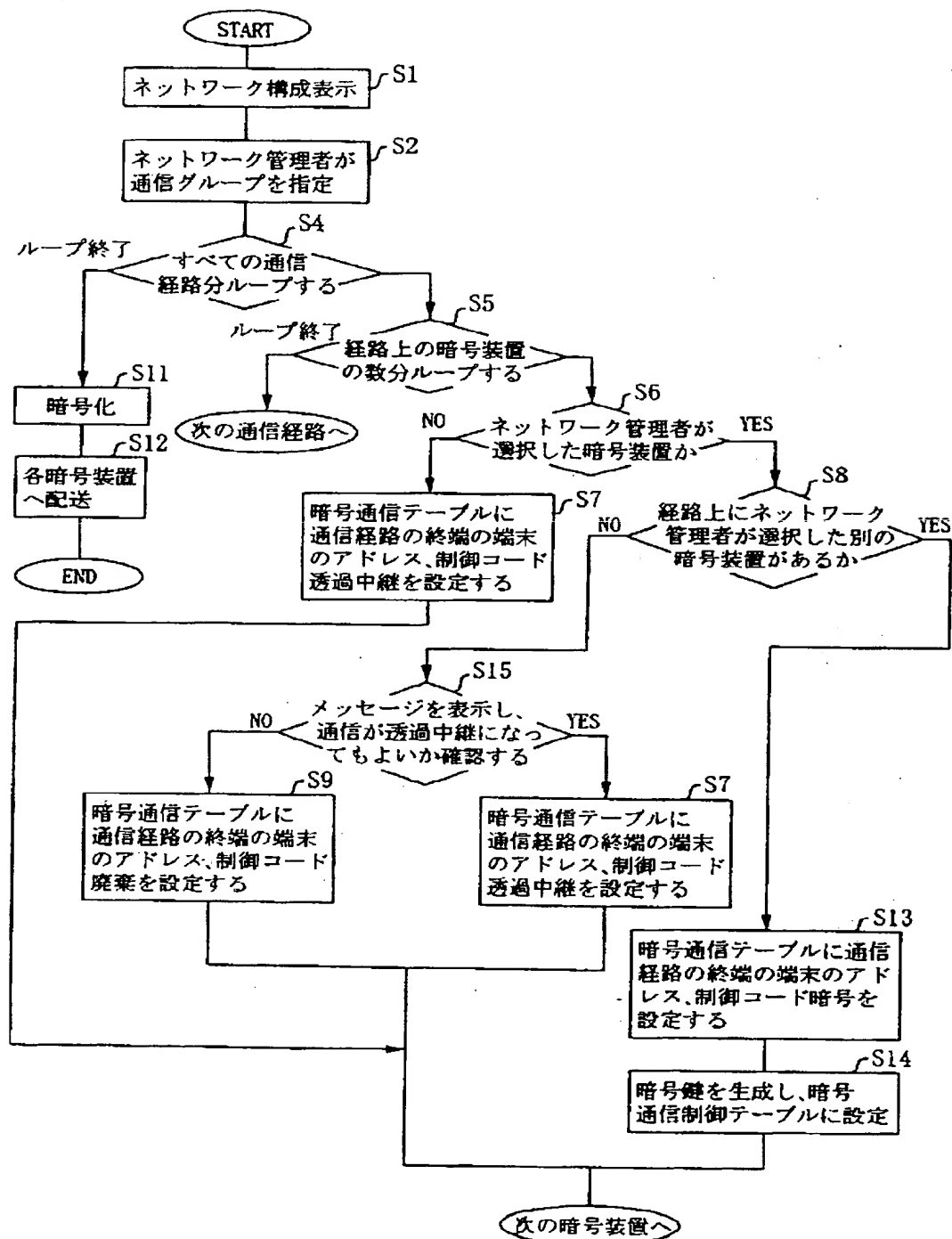
【図13】



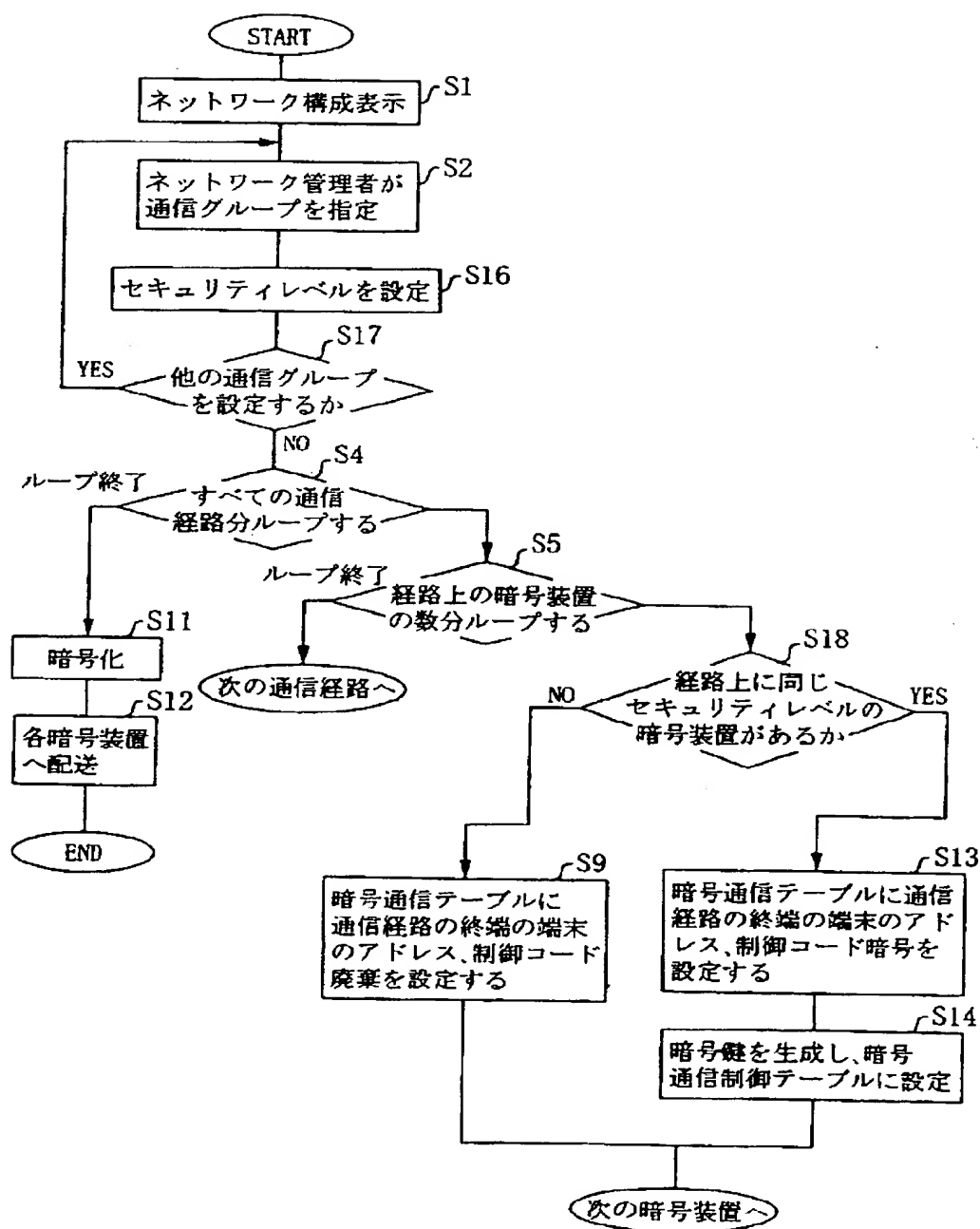
【図15】



【図12】



【図14】



フロントページの続き

(51)Int. Cl.⁶

H 0 4 L 9/36

12/66

12/56

識別記号

F I

H 0 4 L 11/20

B

1 0 2 D

(72)発明者 渡邊 晃
東京都千代田区丸の内二丁目 2 番 3 号 三
菱電機株式会社内

THIS PAGE BLANK (USPTO)